Doc Code: AP.PRE.REQ

PTO/SB/33 (11-08)
Approved for use through 12/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
20423-07775

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed name _____

Application Number	Filed
10/612,198	July 1, 2003

First Named Inventor
Carey S. Nachenberg

Art Unit	Examiner
2137	Zachary A. Davis

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☑ attorney or agent of record.
Registration number 39,713

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Brian Hoffman/
Signature

Brian M. Hoffman
Typed or printed name

415-875-2484
Telephone number

December 10, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ATTACHMENT TO THE PRE-APPEAL BRIEF REQUEST FOR REVIEW

Pre-appeal review is requested because the rejections of record are clearly improper and without any factual or legal basis. Applicants respectfully request that the panel reconsider and lift the rejections of record.

I. Status of Claims

Claims 1, 3, 4, 6-11, 13-16, 18-20 and 22-24 are pending and stand finally rejected. Claims 2, 5, 12, 17 and 21 are canceled. Claims 1, 3, 4, 6-11, 13-16, 18, 19, 21, 23 and 24 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Applicant admitted prior art, in view of Ramarao (U.S. Publication No. 2004/0199647) and in further view of Gruper (U.S. Patent No. 7,047,369). Claim 20 stands rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Applicant admitted prior art, in view of Ramarao, in view of Gruper and in further view of Yaeger (US Patent No. 5,768,422). Claim 22 stands rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Applicant admitted prior art in view of Ramarao, in view of Gruper and in further view of Yaeger.

II. Status of Amendments

Appellant filed an Amendment After Final on October 27, 2008 amending the specification and canceling claim 21. In the Advisory Action of November 14, 2008, the Examiner indicated that these amendments are entered for purposes of appeal.

III. Claim 23 is not Obvious in View of the Cited References

The Examiner rejects claim 23 under 35 U.S.C. § 103(a) as being unpatentable over Applicant admitted prior art, in view of Ramarao and in further view of Gruper. The admitted prior art, Ramarao and Gruper, either alone or in the combinations suggested by the Examiner, do not teach or suggest every limitation of claim 23. Claim 23 depends from independent claim 1. Independent claim 1 recites elements related to training a database intrusion detection system. For example, independent claim 1 recites:

observing, in real time, commands that are accessing the database during a training phase;
grouping the commands into categories;
performing a statistical analysis of the categories;
deriving from said commands, in real time, a set of acceptable commands; and
ending the training phase responsive to the statistical analysis.

Thus, independent claim 1 recites, *inter alia*, "grouping the commands into categories…," "performing a statistical analysis of the categories," deriving "a set of acceptable commands" and "ending the training phase responsive to the statistical analysis."

Claim 23 incorporates the limitations of independent claim 1 and recites that the computer-implemented method of training a database intrusion detection system in real time further comprises:

establishing new categories responsive to the observed commands, and wherein:
the statistical analysis determines whether a predetermined threshold number of the new categories has been exceeded; and
the training phase ends responsive to a determination that the predetermined threshold number has been exceeded.

Thus, claim 23 recites observing commands accessing a database during a training phase and establishing new categories of commands responsive to the observed commands.

The cited references, whether considered alone or in the combinations suggested by the Examiner, do not teach or suggest "observing, in real time, commands that are accessing [a] database during a training phase…" and "establishing new categories responsive to the observed commands…" as recited in claim 23. The admitted prior art merely discloses the existence of database intrusion detection systems. *See* Spec., p. 1, lines 4-17. Ramarao, in turn, describes a software environment in which a message requesting an action is received from a node. A determination is made that the action is not permitted in the software environment and the requested action is prevented from occurring. *See* Ramarao, Abstract. However, Ramarao does not teach or suggest observing commands that are accessing a database during a training phase and establishing new categories of commands responsive to the observed commands.

The Examiner points to ¶ [0032] in Ramarao as disclosing establishing new categories of commands responsive to observed commands. *See* Final Office Action (8/25/08), p. 8. This

portion of the reference discloses that multiple nodes can exist in a client environment and that access control software can be implemented against each node in the client environment to restrict one node from initiating remote actions and/or operator initiated actions onto another node. The disclosed access control restrictions can be granular, and can be set based on parameters to the remote actions:

> Additionally, the enforcement can be made granular in terms of what exact remote actions can be initiated. The parameters to those remote actions can be set to be validated, if they can be compared against any local OVO environment variable, string matched, or just **configured as variable**. In one embodiment, only the actions that are defined in the configuration file of access control software 460 are allowed, all other actions are prevented from occurring.

(Ramarao, ¶ [0032], emphasis added). Thus, at most Ramarao may disclose that parameters for access control restrictions for a given node can be configured as variable. However, Ramarao does not disclose observing commands that are accessing a database, much less observing commands that are accessing a database during a training phase and establishing new categories of commands responsive to the observed commands. Instead, Ramarao teaches the use of a pre-specified access controls. Thus, Ramarao does not teach or suggest "observing, in real time, commands that are accessing [a] database during a training phase" and "establishing new categories responsive to the observed commands" as recited in claim 23.

Gruper does not remedy the deficiencies of Ramarao. Gruper describes an operating environment that prevents unacceptable application behavior by defining activity behavior as either acceptable or suspect. *See* Gruper, Abstract. However, Gruper does not teach or suggest observing commands that are accessing a database during a training phase and establishing new categories of commands responsive to the observed commands.

The Examiner argues that Gruper discloses establishing new categories of commands responsive to observed commands at 5:32-61. This portion of the reference describes a learn mode as follows:

> In this mode a new program is assigned a general enforcement file. The general enforcement file gives the program no access rights at all to files on the system disk. The program then attempts to make a file access. Provided the

> attempt is within certain parameters **the system allows the attempt and learns the details** so that in (sic) future an access to that area of the disk will always be allowed. **Thus an enforcement file is gradually built up over the duration of the learn mode**. The specific enforcement file is then consulted, in future access attempts, to decide whether the program has rights to access the required part of the system disk at the required level.

(emphasis added). Thus, Gruper discloses building a specific enforcement file for a new program by observing and recording program disk accesses. The enforcement file is consulted in future accesses to determine whether to allow a particular disk access by the program.

However, Gruper does not teach or suggest that new categories are established responsive to the learned access details. Grouper simply builds the enforcement file; it does not categorize the learned accesses. Even if one were to argue that Grouper establishes a separate category for each program for which access rights are learned, such categories would be pre-established before the learning begins. The "categories" would not be established "responsive to the observed commands" as claimed. Thus, Gruper does not teach or suggest "establishing new categories responsive to" observed commands as recited in claim 23.

In addition, Gruper does not perform a statistical analysis of new categories to determine "whether a predetermined threshold number of the new categories has been exceeded" as claimed. The Examiner points to Gruper, 2:50-63 as disclosing this element. *See* Final Office Action (8/25/08), p. 3 and p. 8. This portion of the reference is as follows:

> "In embodiments the step of querying may only be carried out for **a limited period of time**. This may be literally a predetermined time from installation of any given program or it may be a predetermined time measured only whilst the new program is running. Alternatively a program may be run in this learning mode until the next occasion upon which the computer is reset. Then again in one embodiment **a predetermined number of operations of the new program is counted through**, and once that number is reached learning mode is ended. Other forms of limitation of the learning mode will suggest themselves to the skilled person and all of these are viable alternatives that could provide useful embodiments of the invention. As an alternative it is possible not to set a limit on the length of the learning mode."

(emphasis added). The text relied upon by the Examiner describes multiple ways of ending the learning mode. Several of the ways are dependent upon only elapsed time, and cannot reasonably be said to involve a statistical analysis of categories or determining that a predetermined threshold number of new categories has been exceeded. Another way of ending the learning mode is waiting until the computer "is reset" and this method also does not involve a statistical analysis of categories or determining that a predetermined threshold number of new categories has been exceeded. The final way of ending the learning mode disclosed in the portion cited by the Examiner is counting a "predetermined number of operations" and this technique must be the alleged statistical method referenced by the Examiner. Thus, at most Gruper may disclose a statistical analysis determining that a predetermined number of operations has been exceeded. However, Gruper does not teach or suggest a statistical analysis of categories, much less a statistical analysis determining that a predetermined threshold number of new categories has been exceeded.

Accordingly, Appellants respectfully submit that the cited references do not teach or suggest every element of claim 23. Therefore, a person of ordinary skill in the art would considering the references either individually or in combination would not find the claimed invention obvious. For this reason, Appellants request that the Panel overturn the rejection of claim 23.

Respectfully submitted,

CAREY NACHENBERG ET AL.

Dated: December 10, 2008

By: /Brian Hoffman/
Brian M. Hoffman, Reg. No. 39, 713
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (415) 875-2484
Fax: (415) 281-1350